

PCT

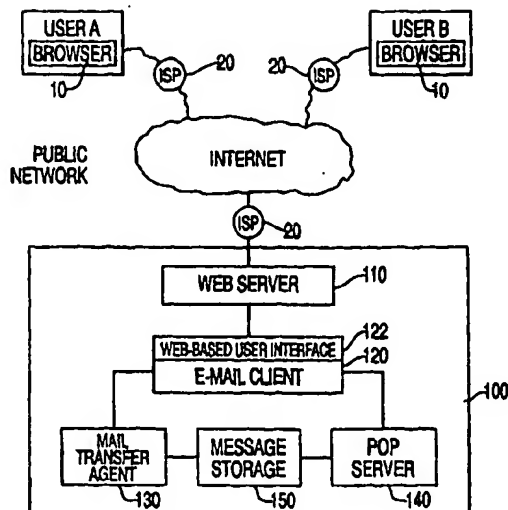
WORLD INTELLECTUAL PROPERTY ORGANIZATION  
International Bureau



INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification <sup>6</sup> : <b>H04L 12/00</b>	<b>A2</b>	(11) International Publication Number: <b>WO 00/02348</b> (43) International Publication Date: 13 January 2000 (13.01.00)
(21) International Application Number: PCT/US99/15029 (22) International Filing Date: 1 July 1999 (01.07.99) (30) Priority Data: 60/091,484 2 July 1998 (02.07.98) US (71) Applicant: MAIL.COM, INC. [US/US]; Suite 660, 11 Broadway, New York, NY 10004 (US). (72) Inventors: KASHPUREFF, Eugene, E.; 1116 Woodmere Place, Plainfield, NJ 07062-2226 (US). WALDEN, Charles, R., Jr.; 43 Glenwood Road, Montclair, NJ 07043 (US). (74) Agent: MILLER, Joel; 17 Westwood Drive South, West Orange, NJ 07052-1822 (US).		(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).  Published <i>Without international search report and to be republished upon receipt of that report.</i>

(54) Title: SECURE WEB-BASED MAIL AND AUTHENTICATION SYSTEM



(57) Abstract

Electronic mail ("e-mail") messages and attachments can be sent securely via the Internet by using a web-based e-mail system under a secure protocol. The sender logs onto the web-based e-mail system under the secure protocol and sends or composes the message for the recipient. The recipient then logs onto the system and retrieves or reads the message over a secure link. Confirmation of secure transmission over the Internet and authentication of the sender's identity or e-mail address can be provided by recording secure-transmission status and authentication within the system.

**FOR THE PURPOSES OF INFORMATION ONLY**

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece	ML	Mali	TR	Turkey
BG	Bulgaria	HU	Hungary	MN	Mongolia	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MR	Mauritania	UA	Ukraine
BR	Brazil	IL	Israel	MW	Malawi	UG	Uganda
BY	Belarus	IS	Iceland	MX	Mexico	US	United States of America
CA	Canada	IT	Italy	NE	Niger	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NL	Netherlands	VN	Viet Nam
CG	Congo	KE	Kenya	NO	Norway	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NZ	New Zealand	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	PL	Poland		
CM	Cameroon	KR	Republic of Korea	PT	Portugal		
CN	China	KZ	Kazakhstan	RO	Romania		
CU	Cuba	LC	Saint Lucia	RU	Russian Federation		
CZ	Czech Republic	LI	Liechtenstein	SD	Sudan		
DE	Germany	LK	Sri Lanka	SE	Sweden		
DK	Denmark	LR	Liberia	SG	Singapore		
EE	Estonia						

- 1 -

## SECURE WEB-BASED MAIL AND AUTHENTICATION SYSTEM

### Technical Field and Background Art

5           This application claims the benefit of U.S. Provisional Application no. 60/091,484, filed July 2, 1998.

          It is a well known fact that the Internet is not secure. Send information via the Internet, and you run the risk of having others intercept it. To prevent this, encryption  
10       systems have been devised to shield the information from all but the sender and the intended recipients. Although such measures accomplish the desired goal, they require the installation of special software on both the sender's and recipient's computers. Further, the complexity of the software occasionally prevents the completion of a secure channel.

15       Additionally, mail headers in messages can be forged, permitting unauthorized assumption of others' identities. When such messages are received, the recipient has no readily-available means of determining the authenticity of the purported identities.

### Brief Description of Drawings

20       Figures 1-3 are block diagrams of a secure web-based mail system;  
          Figure 4 is a flowchart of the method of acquiring a secure mail channel;  
          Figure 5 is a flowchart of the method of authenticating the identity of the sender;  
          and  
          Figure 6 is a block diagram of a secure mail system with multiple web-based e-  
25       mail systems.

### Modes for Carrying Out the Invention

          By creating a secure connection between an Internet user and a web-based electronic mail provider, mail and any attachments or other data can be sent by the  
30       originator securely without the need for additional software, such as an encryption package (e.g., PGP) or a specialized electronic mail software package (e.g., Eudora).

- 2 -

The recipient retrieves the mail through a secure connection to the same electronic mail provider, insuring that the mail remains confidential. Additionally, messages sent through the web-based electronic mail provider can be authenticated by virtue of a secure log-in process.

5           A system for secure mail transmission is illustrated in the block diagram of Figure 1. Users A and B are computers with browsers 10 that interact with a network-based messaging system, such as a web-based electronic mail (or "e-mail") system 100 through a public, on-line electronic communications network, such as the Internet or some other network. The web-based e-mail system 100 may comprise a  
10   web server 110, an e-mail client 120 having a web-based user interface 122, a mail transfer agent or MTA 130 (such as an SMTP server), a mail server such as a POP (post office protocol) server 140, and a message storage device 150. Users A and B and the web-based e-mail system 100 typically connect to the Internet through Internet service providers or ISPs 20.

15           To obtain a secure communications link, the web-based e-mail system 100 invokes a secure protocol, such as secure "http" or "https" (hypertext transport protocol under SSL or secure socket layer; see, e.g., U.S. Patent No. 5,657,390, titled "Secure socket layer application program apparatus and method," incorporated herein by reference), SSH (secure shell), PCT (Microsoft's private communications technology),  
20   TLS (transport layer security), or some other protocol that provides a secure connection.

          Software for the desired protocol could reside in the web server 110. The user requires only a protocol-compatible software package device such as a conventional web browser (e.g., Netscape Communicator or Microsoft Internet Explorer); no  
25   additional software or hardware is required. The web-based e-mail system 100, in concert with the browser, creates an encrypted channel or link between the user's browser and the web server 110 using the routine determined by the protocol. In the case of SSL, a secure session is started by changing the protocol from "http" to "https."

          A secure connection may be created at any one of the following points: (1) prior  
30   to or immediately upon log-in to the e-mail service, either automatically or at the user's request; (2) when an e-mail message is composed, again either automatically or at the

- 3 -

user's request; or (3) automatically based upon a user or subscriber profile. The point at which the secure connection is created may be chosen to suit the application and is a matter of design choice; the secure connection could be created at times and in ways other than those mentioned, as well, if desired.

5           Initially, a user connects to the Internet and logs onto the web-based e-mail service, resident in the web-based e-mail system 100. Optionally, the user can enter a password when requested to do so, and the server can verify the identity of the user, based on previously-stored information. The user can then select from options including reading and sending mail. Additionally, if the user's profile so provides, a  
10       secure connection is automatically established using https or some other protocol, or, if the system is so configured, the user may request a secure connection if one does not exist.

          If the user desires to create and send a message in a secure fashion, the user first requests a secure connection and, if one does not already exist, the system  
15       invokes the appropriate protocol. Then, the user composes the message and the message is sent. A configuration that will accomplish the foregoing is illustrated in Figure 2, showing a secure link 30 between the browser of user A and the web-based e-mail system 100. A method for achieving this is outlined in the left-hand column of the flowchart of Figure 4.

20           The message may contain text, data, graphics, audio, and/or video. By virtue of the secure link 30, user A functions as a virtual remote terminal communicating with the web-based e-mail system 100 via the Internet under the secure protocol.

          The recipient or recipients of the message (user B, user C, etc.) connect to the Internet and then log onto the web-based e-mail system 100. Again, the identity of the  
25       recipient may be confirmed by a password or some other device. If mail generated under the secure protocol is present for the recipient(s), a secure link 30 between the recipient(s) and the web-based e-mail system 100 is established or confirmed, as shown in Figure 3 (an additional secure link to a second recipient, user C, shown dashed), and the mail is retrieved. Here, the recipients are functioning as virtual  
30       remote terminals of the web-based e-mail system 100. A method for accomplishing the retrieval is illustrated in the right-hand column of the flowchart of Figure 4.

- 4 -

The system can be configured to confirm that the message was sent and retrieved under secure conditions as well as authenticate the sender's identity. If the sender is a user of the web-based e-mail service, the sender's e-mail address or other identification information (and, therefore, the sender's identity) is authenticated by the password or some other method of authentication used to enter the e-mail service. If a secure and/or authenticated connection is used when the message is originally sent, the web-based e-mail system 100 can add a secure-transmission/authentication device to the message, such as a tag placed in the message header, upon its arrival at the e-mail system 100. When the recipient logs onto the system and the message is retrieved, the web-based e-mail system 100 could indicate to the recipient that the message was received under secure conditions and could also authenticate the identity or e-mail address of the sender. The secure-transmission/authentication device (such as a tag) can be stripped from the message when the message leaves the web-based e-mail system 100.

A method for confirming the identity of the sender is illustrated in the flowchart of Figure 5. This method can be combined with the method of Figure 4 to provide secure messaging and authentication. It should be understood that these methods may be used independently and that the indicators of secure transmission status and authentication status may be combined or kept separate.

A person masquerading as an authorized user through the use of forged e-mail headers will lack the appropriate authenticating information, and messages originating from the "masquerader" and received over the Internet can be marked as not authenticated or, in the alternative, blocked.

In lieu of a secure-transmission/authentication device or tag, the web-based e-mail system 100 could utilize a look-up table or database, cross-referencing each message with its secure (or non-secure) and/or authenticated (or not authenticated) status. Whenever a message is sent or retrieved, the table or database would be consulted regarding the status and proper handling of the message, and updated if necessary.

The system of Figure 1 can be expanded to incorporate multiple, third-party web-based e-mail systems 200, each with its own users (x and y), as shown in Figure 6.

- 5 -

There, the web-based e-mail system 100 is connected to a third-party web-based e-mail system 200 by a secure link, such as a leased or dial-up telephone line or fiber optic cable 210, encrypted if necessary, or an encrypted channel 220 over the Internet. Since each of the systems 200 implement similar policies of secure connection and user authentication, the benefits of secure transmission and authentication provided by a single system 200 is expanded across multiple systems.

Where third-party web-based e-mail systems 200 are interconnected with the primary web-based e-mail system 100, the third-party system 200 could confirm the secure status of a message by the presence of an secure-transmission device and receipt of the message via a secure link. Alternatively, the secure status of a message could be determined by use of a shared look-up table or database.

By interconnecting two or more web-based e-mail systems through secure links, an expanded universe of security is created. Messages can then pass between the systems and its users in secure fashion, with indicia of secure status (e.g., a security device or tag).

- 6 -

What is claimed is:

1. A system for communicating over a public on-line electronic communications network, comprising:

at least one user, each user comprising means for sending and retrieving  
5 messages over the network;

a network-based messaging system; and

means for selectively establishing a secure connection between the messaging system and a user.

10 2. A system as set forth in claim 1, where the network is the Internet and the network-based messaging system is a web-based electronic mail system.

3. A system as set forth in claim 2, where the web-based electronic mail system comprises a web server and an e-mail client with a web-based user interface,  
15 and the user comprises a web browser.

4. A system as set forth in claim 2, where the web-based electronic mail system comprises a web server, an e-mail client with a web-based user interface, a mail transfer agent, and a mail server.

20

5. A system as set forth in claim 1, where the means for selectively establishing a secure connection comprises means for establishing a secure hypertext transfer protocol connection.

25 6. A system as set forth in claim 1, further comprising means for retrieving the message from the network-based messaging system over the public on-line electronic communications network via a secure connection.

30 7. A system as set forth in claim 1, further comprising means for providing an indication of secure-transmission of the message.

- 7 -

8. A system as set forth in claim 1, further comprising means for providing an indication of authentication of the identity of the user.

5 9. A system as set forth in claim 1, further comprising at least one third-party network-based messaging system and means for establishing a secure connection between the network-based messaging systems.

10 10. A system for securely sending an e-mail message over the Internet, comprising:

means for sending a message via a secure connection over the Internet using a web-based e-mail system; and

means for retrieving the message via a secure connection from the e-mail system over the Internet.

15 11. A system for authenticating the sender of a message to a network-based messaging system over a public on-line electronic communications network, comprising:

means for requesting user-identification and a password from the sender;

means for logging in the sender to the network-based messaging system;

20 means for generating an authentication device based on the identity of the sender; and

means for associating the authentication device with the message.

25 12. A system as set forth in claim 21, further comprising means for establishing a secure connection between the messaging system and the sender.

13. A method of transmitting secure messages, comprising the step of sending a message to a network-based messaging system over a public on-line electronic communications network via a secure connection.

30

- 8 -

14. A method as set forth in claim 10, where step of sending comprises the step of creating a secure connection.

15. A method as set forth in claim 11, where step of creating a secure  
5 connection comprises the step of invoking a secure protocol.

16. A method as set forth in claim 10, further comprising the step of providing an indication of secure-transmission of the message.

10 17. A method as set forth in claim 10, further comprising the step of providing an indication of authentication of the identity of the user.

18. A method as set forth in claim 10, further comprising the step of retrieving the message from the network-based messaging system over the public on-line  
15 electronic communications network via a secure connection.

19. A method as set forth in claim 14, where step of retrieving comprises the step of creating a secure connection.

20 20. A method as set forth in claim 15, where step of creating a secure connection comprises the step of invoking a secure protocol.

21. A method of retrieving secure messages, comprising the step of retrieving a message from a network-based messaging system over a public on-line electronic  
25 communications network via a secure connection.

22. A method of securely sending an e-mail message over the Internet, comprising the steps of:  
sending a message over the Internet via a secure connection using a web-based  
30 e-mail system; and

- 9 -

retrieving the message from the web-based e-mail system over the Internet via a secure connection.

23. A method of authenticating the sender of a message to a network-based messaging system over a public on-line electronic communications network, comprising the steps of:
- requesting user-identification and a password from the sender;
  - logging in the sender to the network-based messaging system;
  - generating an authentication device based on the identity of the sender; and
  - associating the authentication device with the message.

24. A method as set forth in claim 19, further comprising the step of establishing a secure connection between the messaging system and the sender.

1/5

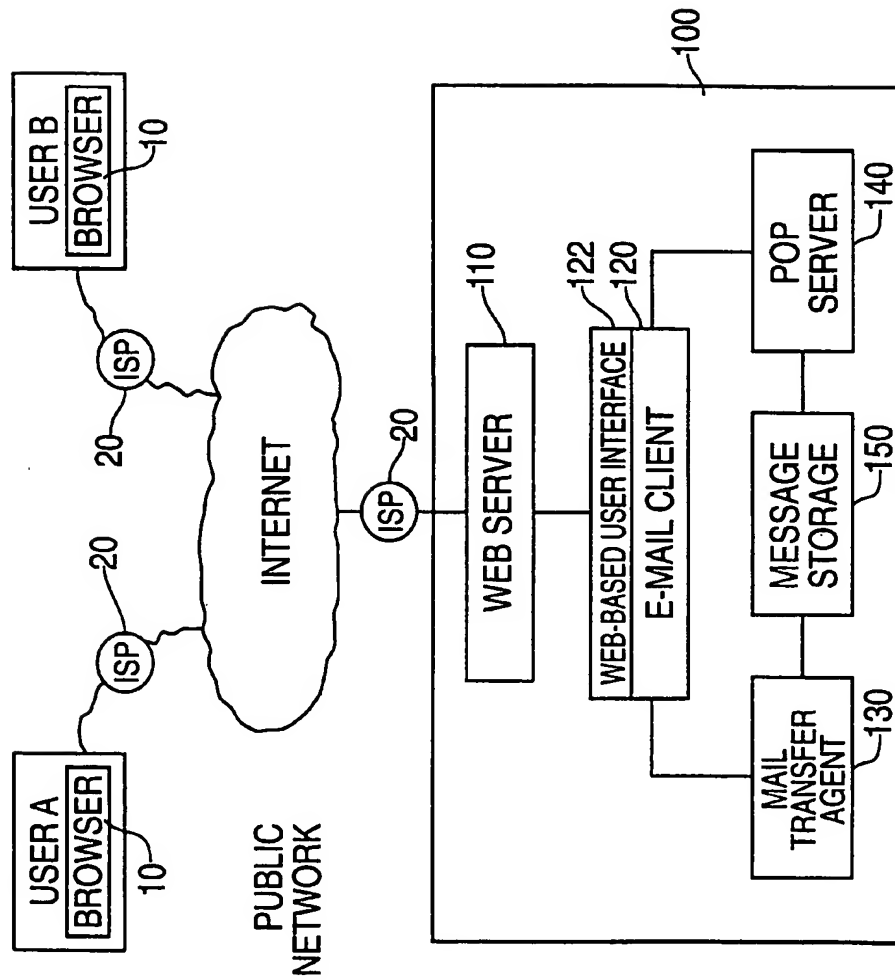


FIG. 1

2/5

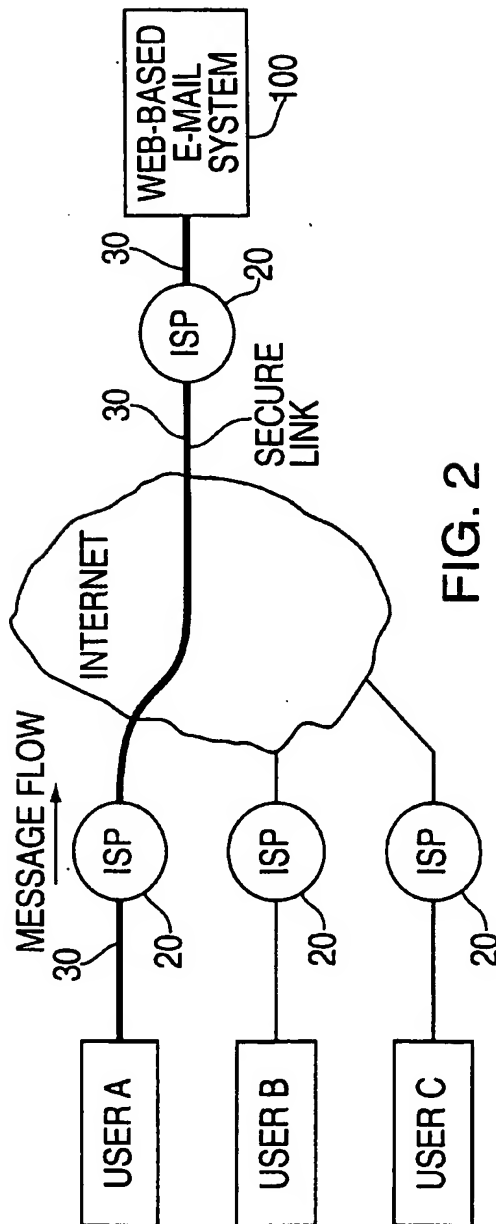


FIG. 2

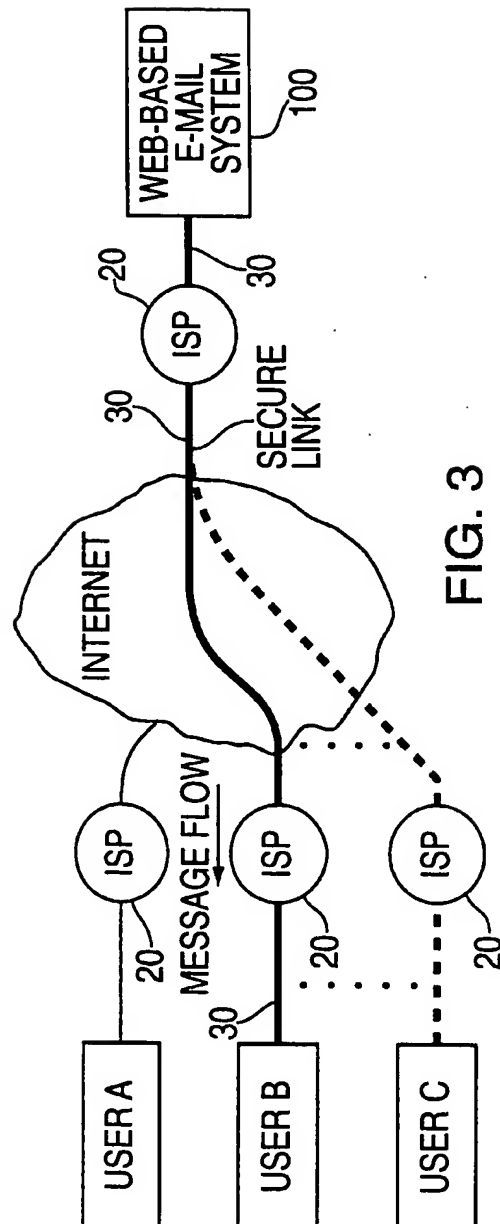


FIG. 3

3/5

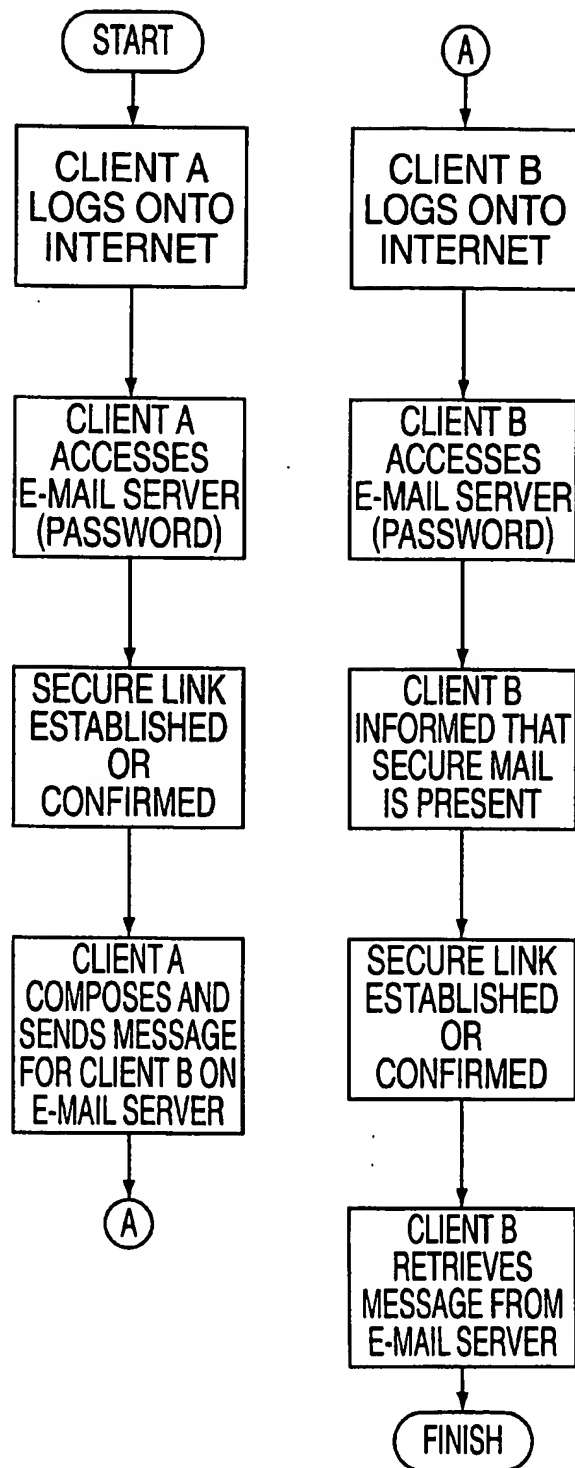


FIG. 4

4/5

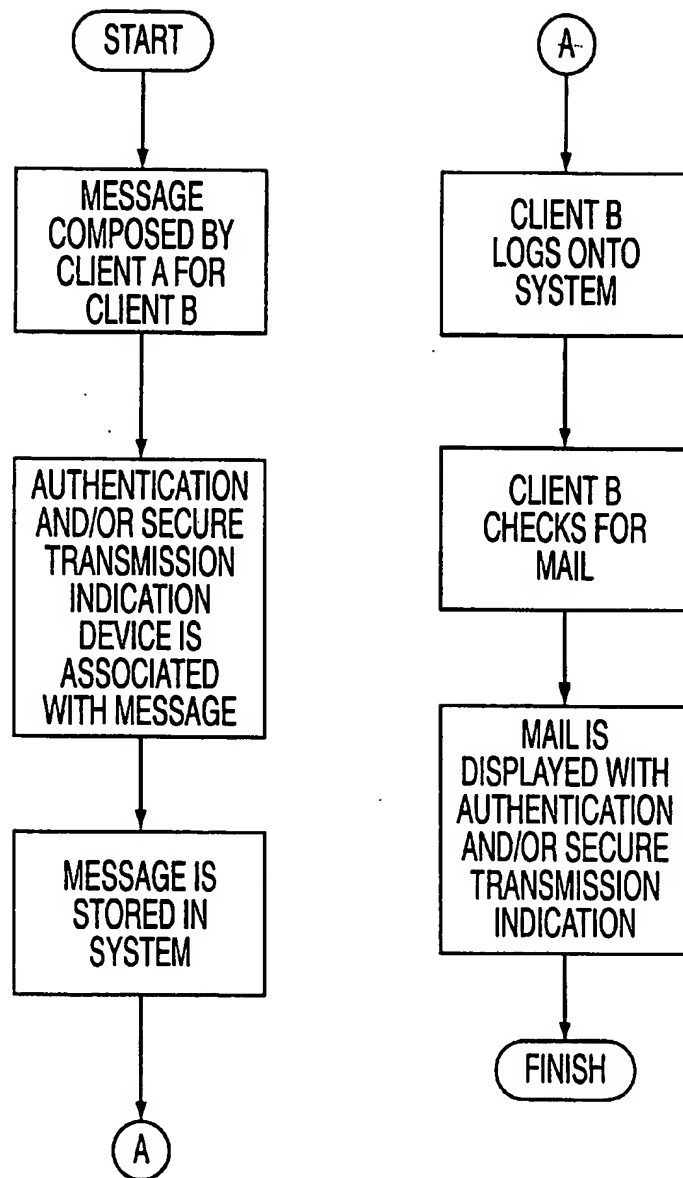


FIG. 5

5/5

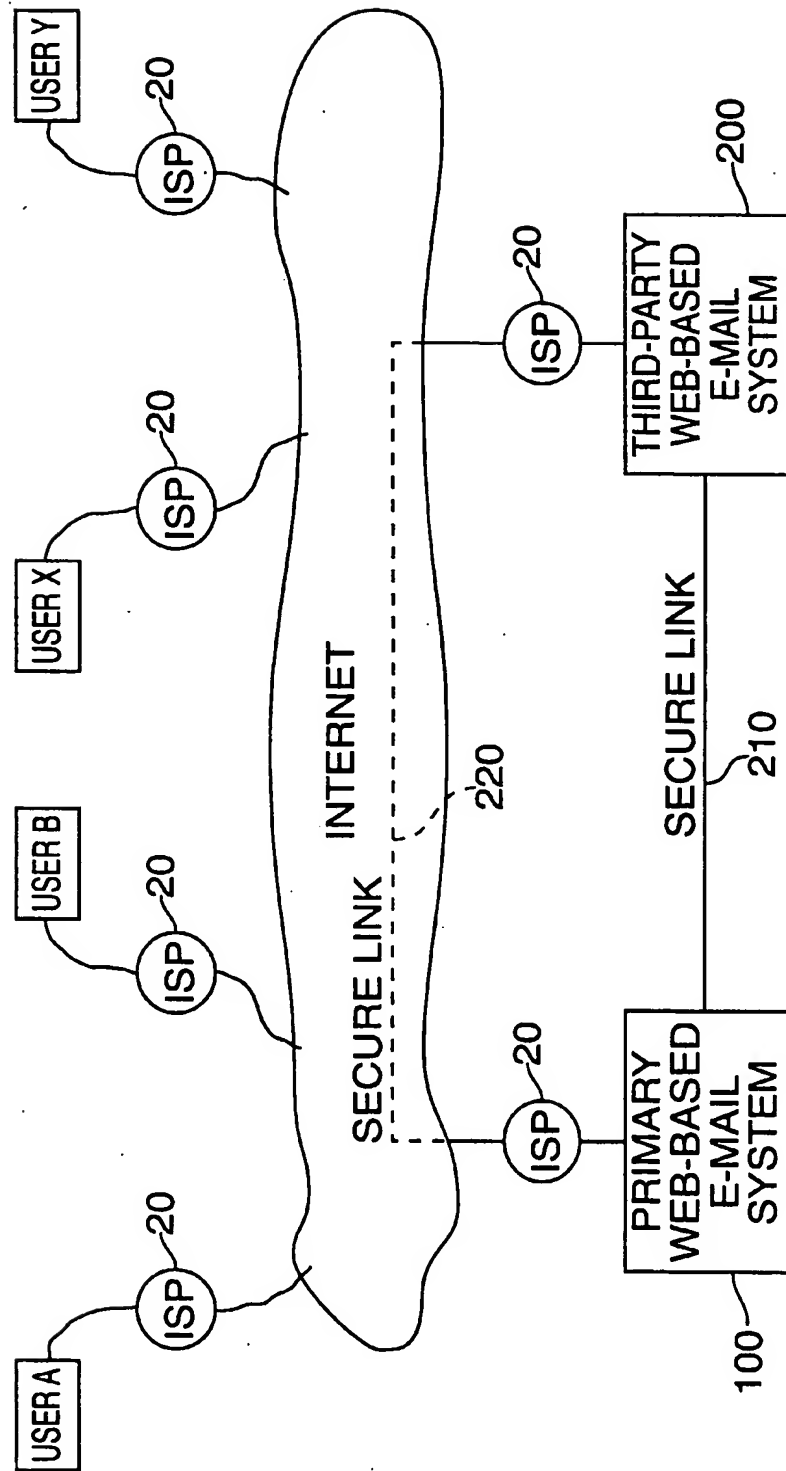


FIG. 6